35010/097

REMARKS

Claims 1-44 are currently pending in the application. Claims 1-44 stand finally rejected. Claims 1, 12-14, 20, 22-25, 31, 33, 34, 36, and 44 are amended herein.

The enclosed amendments introduce no new matter, and do not require additional searching. Accordingly, Applicants respectfully request that the amendments after final be entered and considered.

A telephone conference was conducted on June 23, 2003, between Applicant's attorney Gregg Jansen, Examiner Michael Simitoski, and Supervisor Greg Morse. The discussion centered on independent claim 34 of the patent application. Below is a summary of the discussion of the telephone conference. No agreement was reached.

Issue: Whether Lumsden discloses authentication information.

Supervisor Morse started out by stating that a definition of authentication provided from the field of cryptography concerns certainty of a source of a communication or certainty that the received information has not been changed (citing "Applied Cryptography" by Bruce Snyder). Supervisor Morse and Examiner Simitoski asserted that the transponder identification code of Lumsden comprises authentication information.

Attorney Jansen stated that the identifier code of Lumsden is hardwired into the transponder, citing col. 2, lines 48-50 of Lumsden. Attorney Jansen noted that the hardwired nature of the transponder identification code does not allow changing a digital value in a memory and would prevent the tampering that is the subject of the current application. Attorney Jansen noted that the application defines authentication data as one or more of identification, calibration, or configuration data, and cited page 3, lines 17-20 of the present application. Attorney Jansen stated that Lumsden does not disclose any configuration or calibration data, and does not teach or suggest that a transponder transmit any calibration or configuration data to a central computer.

35010/097

Issue: Whether Lumsden performs a comparison of authentication information to initial information.

Supervisor Morse and Examiner Simitoski stated that Lumsden performs an equivalent comparison when an electrical power measurement is compared to previous electrical power measurements, wherein some manner of alarm or signal was triggered when electrical power use exceeded a threshold.

Attorney Jansen agreed that Lumsden performs comparisons of electrical power measurements. However, Attorney Jansen replied, the electrical power measurements are distinguishable from authentication information and initial information, and are further distinguishable from configuration and calibration information. The comparison of Lumsden does not cause detection or signaling of a tampering occurrence.

Supervisor Morse and Examiner Simitoski also asserted that the comparison in Lumsden of a transponder identification code is the same as the comparison of the present application.

Attorney Jansen replied that Lumsden uses transponder identification codes for transmitting and receiving communications. Attorney Jansen stated that the comparison is not the same, and the comparison cannot detect tampering.

Issue: Whether Lumsden discloses tampering.

Supervisor Morse argued that Lumsden discloses tampering. Supervisor Morse based this line of reasoning on Examiner Simitoski's rejection. Examiner Simitoski's previous rejection relied on a dictionary definition of tampering that included "tinkering". Supervisor Morse stated that a consumer in Lumsden committed tampering by using electrical power beyond a prescribed level, wherein such excessive power use was abnormal, thereby comprising tampering. Supervisor Morse concluded that because the power company in Lumsden was trying to prevent excessive electrical power usage at normal peak usage times, the consumer was not authorized to use the power and was guilty of tampering.

35010/097

Attorney Jansen inquired whether changes in electrical power measurements can comprise tampering. Attorney Jansen contended that such a definition of tampering would encompass most measurements, and such a definition of tampering would be meaningless, as all actions could comprise tampering. The assertion that the act of exceeding an electrical power threshold comprises tampering is illogical, attorney Jansen stated, as a homeowner is authorized and allowed to change his thermostat.

Supervisor Morse replied that Lumsden teaches that excessive power consumption is to be avoided, and that Lumsden implies tampering because the central computer can cut off electrical power if the threshold is exceeded.

Attorney Jansen replied that the power company has authority to cut off power to a consumer, just as the consumer has the authority to set his thermostat, and therefore using excessive power is not tampering. Instead, Attorney Jansen asserted that tampering comprises some illegal or unauthorized access. Attorney Jansen reiterated the purpose of the invention was to prevent unauthorized modification of calibration and configuration data, wherein the measurement ability of an associated measurement device would be compromised. Attorney Jansen concluded that Lumsden does not teach or suggest preventing unauthorized changes to a signal conditioning circuitry in order to compromise the measurement capability and accuracy of the device.

Issue: Whether the patent application provides a definition of tampering.

Supervisor Morse asserted that the present application does not provide adequate boundaries on tampering. Supervisor Morse asked what tampering is limited to in the application.

Attorney Jansen replied that tampering in the context of the patent application comprises requesting and receiving authentication information, comparing it to initial information, and signaling a tampering condition if the authentication information is not equal to the initial information, i.e., detecting whether specific information has been changed.

35010/097

The Office Action asserts that the IDS filed on March 5, 2004 was not considered, as a concise explanation of the single prior art reference listed in the IDS was not provided. Applicants filed the IDS because the Chinese publication 1166199A was provided to Applicants in a Chinese office action, and shows what appears to be a Coriolis flow meter (see FIGS 1 and 1A).

Claims 1, 12, 23, and 34 stand rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. The Office Action asserts that the limitation that the host signals a tamper condition in the signal conditioning circuitry was not disclosed in the patent application. Applicants contend that the signaling was fully disclosed, and point to FIGS. 1 and 3 and the accompanying text at page 6, lines 6-30 and page 7, line 25 through page 8, line 24. Applicants also point to page 1, lines 4-10.

Claims 1, 12, 23, and 34 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention. The Office Action asserts that it is unclear how the host will "signal" a tampering condition "in the signal conditioning circuitry". This is a straightforward process known in the art, wherein the host system receives the authentication information, performs the comparison, and signals the error condition. The error condition indicates tampering in the signal conditioning circuitry. The error condition signal can be present in the host system while signaling an error condition in the signal conditioning circuitry. The error condition can be held in the host system, and can also be transmitted to other device. Signals generated by a host system can be available for inspection by an operator or technician, for example. Claims 1, 12, 23, and 34 are amended herein to further clarify the invention and to remove the rejection.

Claims 1-3, 8-9, 34-36, 41, and 43 were rejected under 35 U.S.C. § 102(b) as being anticipated by Lumsden (U.S. Pat. No. 4,338,690). Inasmuch as the rejections apply to the claims as amended, Applicants respectfully traverse the rejection.

35010/097

Independent claims 1, 12, 23, and 34 each require periodically transmitting a request for authentication information from a host system to a signal conditioning circuitry. The authentication information can include identification, calibration, and configuration data (see page 3, lines 16-20). The independent claims further require receiving the authentication information from the signal conditioning circuitry in response to the request. The independent claims further require comparing the authentication information with initial information. The initial information comprises authentication information received from the signal conditioning circuitry in response to detecting the signal conditioning circuitry being connected to the host system (see page 4, lines 20-26). The initial information therefore can comprise an initial version of the authentication information (*i.e.*, it is the first set of authentication information received from the signal conditioning circuitry). The independent claims further require signaling an error condition that indicates tampering in the signal conditioning circuitry. The signaling is in response to the authentication information not being equal to the initial information. Advantageously, the invention provides a system for detecting tampering with a signal conditioning circuitry that is remote from a host system.

Lumsden discloses a system for reporting electrical power usage from a residential power meter to a central computer (see abstract). Lumsden provides a transponder that acts as a simple storage device for utility data. The transponder receives data from a data source and stores it until such data is requested through an external instruction (see col. 3, lines 34-59). Lumsden discloses that the central computer sends commands to these residential power meters over telephone lines (see col. 2, lines 56-59). The commands can specify that a particular meter report its stored power consumption data (see col. 2, lines 21-24). Lumsden also discloses requesting information concerning a load of a particular user and subsequent actions to alleviate excessive loads to that user (see col. 4, lines 44-59). Multiple meters in Lumsden can communicate over a single telephone line. Therefore, a particular power meter is identified by a unique code stored in that meter (see col. 2, lines 48-56), *i.e.*, a message is broadcast by the central computer, but only the transponder specified by an ID code in the broadcast message receives and acts on the message.

35010/097

Lumsden does not teach or suggest signaling an error condition that indicates tampering in the signal conditioning circuitry, with the signaling being in response to the authentication information not being equal to the initial information. The Office Action implies that Lumsden performs some manner of tampering detection by asserting that the "central computer can send a load shed command/alarm/tampering condition to the transponder." This is incorrect. Lumsden does not teach or suggest ANY tampering detection. A close inspection of Lumsden does not reveal the terms "tamper," "authenticate," or "calibrate," or any variations thereof.

The Examiner relies on a dictionary definition of tamper that includes "tinkering." Applicant's dictionary, Webster's New Universal Unabridged Dictionary, deluxe second edition, Dorset & Baber, copyright 1983, defines "to tamper with" as including "to make secret, illegal arrangements with . . . to make corrupt, illegal, etc." Tinkering is defined by the same dictionary as including "the act of mending" and "a clumsy or unskillful worker." No mention is made of performing any illegal or unauthorized actions during tinkering. Applicants contend that the word tamper is well known, and is commonly held to include or imply illegal or unauthorized access to or changes in an object, as in jury tampering, vote tampering, etc. Applicants find the definition of tampering asserted in the Office Action and in the recent telephone conference to be completely without merit.

Lumsden does not disclose any comparison of received authentication information to initial information or any signaling of an error condition if the authentication information is not equal to the initial information. Therefore, the Office Action improperly implies tampering detection in Lumsden when all Lumsden discloses is comparing customer electrical power usage to a predetermined level in order for the central computer to perform load shedding actions.

In addition, Lumsden does not teach or suggest comparing authentication information to initial information. Lumsden discloses two comparison operations. First, Lumsden discloses that the central computer monitors electrical power usage measurements and compares these electrical power usage measurements to predetermined electrical power consumption levels (see col. 1, lines 35-38). Second, Lumsden compares transponder identification codes to known codes in order to regulate electronic communications and identify message transmitters and message

recipients. Neither of these comparing operations, in the greatest stretch of the imagination, can be viewed as detecting or signaling an error condition that includes tampering. Lumsden is incapable of detecting tampering and is incapable of signaling an error condition that indicates tampering.

Lumsden does not teach or suggest requesting or receiving authentication information as in the present application. While Lumsden includes a transponder identification code in communication messages, the transponder identification code does not comprise authentication data as in the present application. Lumsden discloses that the transponder identification code is hard-wired into the transponder (see col. 2, lines 48-50). The term "hard-wired" connotes physical provision or formation of digital data, wherein the digital data is not programmed into a memory, and therefore cannot be tampered with. The hard-wired transponder identification code of Lumsden cannot be reprogrammed and therefore cannot be used for detecting tampering.

For the foregoing reasons, Applicants respectfully request reconsideration and withdrawal of the rejection of claims 1-3, 8-9, 34-36, 41 and 43 under 35 U.S.C. § 102(b) as being anticipated by Lumsden.

Claims 5 and 8 stand rejected under 35 U.S.C. § 103(a) as being obvious over Lumsden in view of U.S. Patent 5,014,038 (Leigh-Monstevens et al.). Claims 5 and 8 depend from independent claim 1 and therefore are patentable for the reasons previously discussed.

Claims 4, 10, 11, 37, 42, and 44 stand rejected under 35 U.S.C. § 103(a) as being obvious over Lumsden in view of U.S. Patent 6,289,456 (Kuo et al.). Claims 4, 10, 11, 37, 42, and 44 depend from independent claims 1 and 34 and therefore are patentable for the reasons previously discussed.

Claims 6 and 7 stand rejected under 35 U.S.C. § 103(a) as being obvious over Lumsden in view of U.S. Patent 4,933,668 (Oyer). Claims 6 and 7 depend from independent claim 1 and therefore are patentable for the reasons previously discussed.

35010/097

Claims 39 and 40 stand rejected under 35 U.S.C. § 103(a) as being obvious over Lumsden in view of Leigh-Monstevens and Oyer. Claims 39 and 40 depend from independent claim 34 and therefore are patentable for the reasons previously discussed.

Claims 12-14, 19-20, 23-25, 30, and 31 stand rejected under 35 U.S.C. § 103(a) as being obvious over Lumsden in view of U.S. Patent 6,526,839 (Barger et al.) and further in view of U.S. Patent 3,355,944 (Sipin). Applicants respectfully traverse the rejection.

The rejection reiterates the assertion that Lumsden discloses a meter system as in the present invention, but lacks disclosure of meter electronics for a Coriolis flowmeter. This is incorrect. As previously discussed, Lumsden does not disclose comparing an authentication information to an initial information and does not disclose signaling an error condition. Therefore, the combination of Lumsden, Barger, and Sipin does not provide a system that detects an error.

Applicants respectfully request reconsideration and withdrawal of the rejection of claims 12 and 23 under 35 U.S.C. § 103(a) as being obvious over Lumsden, Barger, and Sipin. Claims 13-14, 19-20, 24-25, and 30-31 depend from independent claims 12 and 23 and therefore are patentable for the reasons previously discussed.

35010/097

In light of the foregoing amendments and remarks, Applicants believe that pending claims 1-44 are in condition for allowance, and that action is respectfully requested. If there are any remaining matters that can be handled in a telephone conference, the Examiner is invited to telephone the undersigned attorney, Gregg Jansen, at (303) 938-9999 ext 14.

Respectfully submitted,

Date: 6/24/04

Gregg L. Jansen, Reg. No. 46,799
Duft Setter Ollila & Bornsen LLC
Tel.: (303) 938-9999, ext. 14
Fax: (303) 938-9995

Correspondence Address:

Customer No: 32827